Telecommunications companies such as Vodafone, O2 owner Telefonica, and Orange have written a letter to EU and NATO officials warning that an increase in sabotage incidents is jeopardizing critical services.

Open Letter from European Telecommunications Operators and Subsea Cable Stakeholders to the European Union, United Kingdom, and NATO on Subsea Critical Infrastructure Security

At this crucial time for Europe's security and resilience, we commend your efforts to strengthen collective defence and protect critical infrastructure. Subsea cables play a vital role in Europe's connectivity, competitiveness, defence readiness, and economic stability. We recommend the EU/EEA and UK authorities as well as NATO renew their collaboration to address this situation effectively, together with the industry stakeholders from the EU and from the UK.

With the rise in hybrid threats, including incidents affecting subsea cables in the Baltic and North Sea, we emphasize the importance of enhanced, coordinated action to safeguard Europe's cross-border networks. The EU Action Plan on Cable Security provides a clear approach to further increase the resilience and security of subsea cables.

We welcome in particular the reference made to the instrumental aspect of the Connected Europe Facility (CEF), and the willingness of the European Commission to launch a dedicated dialogue with industry notably on the definition of the list of CPEIs, and the need for the deployment of surveillance and protection technologies for submarine cable infrastructure. Instruments of the UK authorities and of NATO could strengthen the momentum if coordinated effectively.

The signatories of this letter are strongly committed to contributing to this dialogue with the EC, the UK and the NATO. Globally to deliver on the Action Plan, it is crucial to engage industry stakeholders and establish a clear roadmap for implementation.

The challenge now is to ensure a high level of security and resilience across Europe building on existing frameworks such as the NIS2 Directive and promoting best practices. The entire subsea cable ecosystem must be regarded as critical infrastructure. It is essential to collectively ensure the appropriate level of security screening, protection, and investments into resilience. The repercussions of damage to subsea cables extend far beyond Europe, potentially affecting global internet and power infrastructure, international communications, financial transactions, and critical services worldwide.

We urge the EU/EEA, UK, and NATO decision-makers to work together closely with EU/EEA and UK industry stakeholders. Harmonised approaches must be developed for the subsea cables ecosystem, aiming to align security objectives with operational feasibility as well as a viable business model and based on proportionate and risk-based best practices, developed in close consultation with industry. These best practices on security could be spread through public procurement, which can be mirrored across likeminded partners and NATO allies.

The EU/EEA, the UK, and NATO must invest in the robust exchange of knowledge and intelligence, as well as shared monitoring and surveillance initiatives, involving all relevant stakeholders to pursue collective and enduring solutions. Stronger public-private cooperation with trusted partners is essential for our effectiveness at managing threats and at developing shared resilience strategies.

Investment in advanced technologies to detect and mitigate damage to subsea cables is critical. Such efforts should be supported by funding instruments such as the CEF, or the European Defence Fund. It is therefore of utmost importance to confirm and increase the budget allocated to digital, including the CEF, in the future MFF, as well as the instruments of the UK government and of NATO.

In parallel, the development of additional routes, both terrestrial and subsea, will enhance redundancy and reduce vulnerability to single points of failure. Such aspects of resilience should be enhanced in the objectives of the CEF.

By partnering with industry, Europe can leverage advanced technologies and expertise to improve situational awareness, enable rapid response and strengthen repair capabilities. Simplifying the permitting process and governance structures will further expedite these necessary security measures.

Subsea cable security must be a cornerstone of broader infrastructure protection efforts. By acting now, we can safeguard the networks that underpin our shared future.

Yours sincerely,

ALCATEL SUBMARINE NETWORKS · GlobalConnect · NKT · orange · Proximus Global · SPARKLE · Telefónica · telenor · vodafone